AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning at page 13, line 8 and ending at page 14, line 1 with the following replacement paragraph:

Note that the transition from equation 4 to equation 5 is possible because the equation is a modulo polynomial. Algebraically, $(x + x_1)^2$ would expand into $x^2 + 2xx_1 + x_1^2$. In the modulo 2 environment, the $2xx_1$ term is equivalent to a zero term, leading to the result in equation 5. Note also that this new slope equation (equation 5) is free of the y-coordinate. It enables point-doublings to be repeated without having to compute the y-coordinate at each intermediate step, and thus, has no multiplication step.

New Approach: $2^n P$	
$P_1 = 2P(x,y)$	$s = x + y/x,\ x_1 = s^2 + s + a$
$P_2 = 2P_1\ (x_1,y_1)$	$g = (x + x_1)^2 / x_1 + (s+1),$ $x_2 = g^2 + g + a,$
$P_3 = 2P_2\ (x_2,y_2)$	$r = (x_2 + x_1)^2 / x_2 + ([[s]]g+1),$ $x_3 = r^2 + r + a$
.....	
$P_{n-1}\ (x_{n-1}, y_{n-1}) = ...$	$q = ...$
$P_n = 2P_{n-1}\ (x_{n-1}, y_{n-1})$	$w = (x_{n-1} + x_{n-2})^2 / x_{n-1} + (q + 1),$ $x_n = w^2 + w + a,$ $y_n = x_{n-1}^2 + (w + 1)\, x_n$